PRESS NOTE

CYBER CRIME UNIT HYDERABAD ARRESTS MASTERMIND BEHIND iBOMMA/BAPPAM PIRACY ECOSYSTEM WHO IS ALSO LINKED TO LARGE-SCALE ONLINE BETTING PROMOTIONS

The Cyber Crime Police, Hyderabad City, have achieved a major breakthrough by arresting the prime accused operating the iBomma/Bappam large-scale movie piracy network, which includes over 65 mirror websites responsible for causing thousands of crores in losses to the Telugu Film Industry. The accused was also found diverting lakhs of users from piracy websites to illegal betting platforms such as 1win, 1xbet, and others — a criminal operation that has led to massive financial exploitation of the public. These arrests are the sequel of comprehensive investigation into the piracy of new Telugu films namely **"Kantara Chapter 1", "Dude", "Mirai"** and etc. which have been uploaded onto the illegal websites: **iBomma/Bappam and its extension websites.**

CASE DETAILS AND INVESTIGATION:

Facts of the case are that received complaint from Anti-Video Piracy Cell, Telugu Film Chamber of Commerce (TFCC). They reported that the piracy websites rao.ibomma.foo, bappam.dev, and about 65 associated mirror domains (collectively known as iBomma/Bappam) are illegally uploading and distributing copyrighted Telugu movies without authorization. These websites host newly released theatrical and OTT films in HD quality, causing massive financial losses to the Telugu film industry.

The complainant stated that the operators frequently change domains, use Cloudflare hosting for anonymity, and attract millions of users, resulting in huge recurring losses to producers, distributors, and exhibitors. He further reported that the administrators of these websites have issued public threats to Telugu film producers, including an intimidating message widely circulated on social media. He requested for investigation, blocking of websites, tracing of the operators, and taking necessary legal action. Basing on the complaint, registered a case in Cr.No.1555/2025 U/s 66C, 66E IT Act; 318(4) r/w 3(5) BNS; 63, 65 Copyright Act and investigated into.

During the course of investigation, the **following persons have been identified as the prime accused**

1. **Ravi Emandi Age: 39 years R/o: IDL Green Hills Road, Hyderabad N/o: Visakhapatnam, Andhra Pradesh State. The accused is Presently a Citizen of Saint Kitts and Nevis Country**
2. **Duddela Shivajee Age: 27 years Occ: Website Developer, R/o. Udayagiri, Nellore, Andhra Pradesh (Arrested on 24-09-2025)**
3. **Susarla Prashanth, Age: 27 years, Occ: Private Job, R/o. Pune City, Maharashtra- N/o Atmakur, Nellore, Andhra Pradesh (Arrested on 22-09-2025)**

CASE HISTORY

CREATION OF IBOMMA WEBSITE

- The accused, **Ravi Emandi**, is a native of Visakhapatnam, Andhra Pradesh. He completed his **B.Sc, Computers**, and later moved to Mumbai where he worked in private companies and completed **MBA**.
- After returning to Hyderabad in **2010**, he established **ER Infotech**, a web services firm specializing in domain registration, hosting, and website development.
- Later as internet access became cheaper and widespread, increasing online content consumption and the popularity of OTT platforms like Netflix and Hotstar.
- **Observing the high demand for online streaming, he conceived the idea of creating a free high-quality movie website, earning revenue through advertisements.**
- Simultaneously, he noticed the rapid growth of online gaming and betting platforms and identified them as highly profitable for advertisement partnerships.
- ***Leveraging his technical expertise in web hosting and development, he created the piracy website iBOMMA in 2019, marking the beginning of his piracy and betting promotion operations.***

HOW IT BECAME FAMOUS

- During the COVID-19 lockdown, people were confined to their homes, work-from-home became the norm, and theatres were closed to prevent public gatherings. To watch new movies, the public had to subscribe to multiple OTT platforms, creating a financial burden for many households.
- At this time, the **iBOMMA website** gained rapid popularity by offering newly released movies in high quality on a single platform **free of cost**.
- Millions of users began visiting the site for entertainment during lockdown restrictions. The website link spread widely through **word of mouth, WhatsApp forwards, and various social media platforms**.
- iBOMMA allowed viewers to watch movies and web series **within 1–2 days of release**, from the comfort of their homes and along with their families.
- ***Its superior video quality compared to other piracy websites and torrent platforms made it highly appealing. As a result, iBOMMA became one of the most popular piracy websites, attracting*** *approximately 5 million users per month**.***

CREATION OF A SOPHISTICATED NETWORK FOR OPERATING THE PIRACY WEBSITES:

- As traffic to iBOMMA increased, regulatory actions by the Piracy Cell and copyright authorities led to the primary domains being repeatedly blocked for public access.
- To evade these blocks, the accused created multiple new domain extensions and frequently shifted the website to foreign servers to remain outside Indian jurisdiction.
- With the surge in user traffic, advertisement revenue from gaming and betting applications rose to crores of rupees. This increased revenue enabled the accused to expand and strengthen his illegal operations.
- He used those funds to build a highly sophisticated network of domains and hosting infrastructures.
- The accused also deployed physical servers in different countries Netherlands, Switzerland to support his platforms and ensure uninterrupted streaming of pirated content.
- These measures made it extremely difficult for law enforcement agencies to trace, block, or shut down his piracy network.

OPERATION OF WEBSITE AND TECHNICAL EXPERTISE OF THE ACCUSED

- The accused, Ravi Emandi, is highly skilled in website design, hosting, and maintenance, with experience creating and managing over 900 websites.
- In 2019, he created the iBomma piracy movie website, and in 2022, he developed the Bappam piracy movie website.
- He purchased physical servers in Amsterdam and Switzerland, which he used to operate the iBomma and Bappam TV websites and their various extensions.
- For all domain registrations, he used the Porkbun domain registrar. According to information from Porkbun, he registered 110 domain names related to the iBomma and BappamTV extensions.
- To further conceal server details and mitigate direct blocking attempts, the accused used Cloudflare services.
- He regularly maintained backup copies of movies on external hard drives with the intention of quickly launching new domain extensions of iBomma and Bappam whenever existing ones were blocked by the Ministry of Information & Broadcasting.
- He also embedded malware within pirated movie files, enabling him to collect data from users who download or stream the content

SOURCE OF PIRATED MOVIES

- The accused is downloading movies from OTT platforms on the first day of its release, using third-party applications designed to bypass digital rights management (DRM) protections.
- He is also acquiring pirated copies of movies by purchasing them from various underground sources, with communications and transactions coordinated primarily through Telegram Application.
- Through the Seizures made from the possession of the accused, about **21,000 movies in his hard disks were identified** ranging from Hollywood to Tollywood including several languages ranging from **The God Father-1972 to OG-2025 spanning Hollywood, Bollywood, and Tollywood content.**

REVENUE GENERATION:

- The accused collaborated with online gaming and betting platforms such as 1win, 1xbet, and others, and strategically diverted users visiting the iBOMMA website to these betting sites. By clicking on the website 2–3 times, users were automatically redirected to these gaming platforms. He placed highly visible pop-ups and advertisements that redirected users to illegal betting applications, thereby earning affiliate commissions based on user clicks, registrations, and deposits.
- In addition, many of these betting sites prompted users to download malicious APK files, which infected their mobile phones and computers. These malicious applications captured sensitive user data, which was later sold to cybercriminals and misused for offences such as digital arrest scams, investment frauds, and unauthorized trading.
- Through this illegal ecosystem of piracy and betting promotions, the accused earned approximately ₹20 crores. With the proceeds, he purchased plots and flats, and maintained a balance of ₹3.5 crores in his bank account, which has now been frozen by the police. Further analysis is underway to trace additional funds held in foreign accounts and cryptocurrency wallets.
- ***To evade Indian law, the accused renounced his Indian citizenship and obtained citizenship of Saint Kitts and Nevis. He frequently travelled to countries such as the Netherlands, Switzerland, USA, Thailand, France, and Dubai to collaborate with gaming and betting application operators.***
- By hosting his servers in foreign locations and running his websites from multiple countries, he made it extremely difficult for law enforcement agencies to trace his activities, identify hosting servers, or gather actionable technical details.
- Police, after analyzing technical information obtained from various domain service providers, internet service providers, and passport authorities, successfully apprehended the accused from an apartment in Green Hills Road, Kukatpally.

The accused was also involved in the following cases of Cyber Crime Police Station, Hyderabad

- 1. FIR NO 1042/2025 U/s 66C, 66E of IT Act, & 318(4) r/w 3(5), Sec 63, 65 of Copy Right Act of Cyber Crime PS, Hyderabad
- 2. FIR NO 1292/2025 U/s 66C, 66E of IT Act, & 318(4) r/w 3(5), Sec 63, 65 of Copy Right Act of Cyber Crime PS, Hyderabad.
- 3. FIR NO 1682/2025 U/s 66C, 66E of IT Act, & 318(4),338 r/w 3(5), Sec 63, 65 of Copy Right Act of Cyber Crime PS, Hyderabad
- 4. FIR No 347/2025 U/s 66C, 66D of IT Act, & 318(4), 319(2), 336(3), 340(2) of BNS and Sec 63, 65 of Copy Right Act of Cyber Crime PS, Hyderabad

IMPACT ON THE PUBLIC

- The iBomma and its associated piracy websites gained massive popularity by offering high-quality Movies, Web Series, and OTT content free of cost. **After the arrest of the iBomma organizer, some sections of the public on social media praised him for providing free entertainment, feeling that their viewing options were reduced. However, the dark and dangerous side of these websites is often ignored. By visiting iBomma, Bappam, and similar piracy portals, the public is exposed to severe risks.**
- ***These websites aggressively push users toward illegal Betting and Gaming platforms, redirecting them through pop-up ads and hidden scripts. Users visiting these piracy sites were automatically diverted to betting applications such as 1win, 1xbet, and others, where they were lured with bonuses, misleading offers, and deceptive promotions. The accused's websites recorded over 5 million users per month, and a significant portion of these users ended up registering on betting platforms, eventually losing substantial amounts of money. Numerous recent cases show that victims of such online betting applications, after losing their hard-earned savings, have fallen into deep debt traps, and in several instances, have even resorted to suicide.***
- Further, these piracy websites frequently prompt users to download APK files or install harmful software. These malicious applications can steal personal data, banking passwords, contacts, photos, and OTPs. Through the malware installed on users' devices, the accused collected personal information, financial details, and private photographs, which were later sold to cybercriminals. This stolen data has been misused in various cybercrimes, including digital arrest scams, investment frauds, identity theft, and unauthorized online trading.
- **In summary, while these piracy sites may appear to offer free entertainment, they expose the public to financial loss, data theft, privacy violations, and life-threatening cyber risks.**

SEIZURES MADE:

1) An amount of Rs 3 Crores seized in accused Bank Accounts
2) Mobile phones-3
3) Laptops -3
4) CPUs-6

5) Seagate HDDs, SSDs, pen drives-15
6) Bank Passbooks -10
7) Cheque books from various banks- 35
8) Debit/credit cards of ICICI, IDFC First, HSBC, IndusInd, DBS, HDFC, AU, Federal Bank, etc.-34

Under the guidance of **Addl. Commissioner of Police, (Crimes), Sri. M. Srinivasulu, IPS,** personal monitoringof**DCP Cyber Crimes**, **Smt. Dara Kavitha**, and under the supervision of **ACsP, Sri R.G Siva Maruti and Sri Jayapal Reddy,**officers of Cyber Crime Unit, Hyderabad, **Sri K Madhusudhan Rao, Inspector of Police, Sri S Naresh Inspector of Police, Sri Mahipal, P. Suresh and Sri T. Vinay Kumar, Manmohan Goud Sub Inspectors of Police, Sri V. Maheshwar Reddy Head Constable,** and other members of the teamplayed a crucial role in apprehending the accused and recovering assets. Their commendable efforts, which dismantled a sophisticated Piracy cybercrime network, are worth rewarding.

PUBLIC ADVISORY:

- Any form of watching pirated content on unauthorized websites amounts to theft and severely impacts the film industry and OTT platforms, causing huge financial losses and harming the livelihood of thousands of technicians, artists, and workers who depend on cinema.
- Additionally, piracy websites often force users to download malicious software and APK files, which can compromise mobile phones and computers, leading to data breaches, theft of personal information, financial fraud, and unauthorized access to sensitive dataputting the public at risk of identity theft, banking fraud, and other cybercrimes.
- The **Anti-Piracy Cell of the Telugu Film Industry** and the **Hyderabad City Police** are working tirelessly to eliminate piracy and dismantle illegal networks.Seperate mechanism was setup to **warn the public, raise awareness about malware risks**, and discourage access to piracy websites to protect citizens from harm.

The Cyber Crime Police urge citizens to use only official OTT platforms and legitimate movie sources, and report any suspicious websites or online activity immediately to the Cyber Crime Helpline 1930 or www.cybercrime.gov.in.

V. C SAJJANAR, IPS
Commissioner of Police,
Hyderabad City.